COT Security Alert – Deadline Approaches for DNSChanger-Infected Hosts

The COT Security Administration Branch sent an alert on May 29, 2012 explaining the reason for the FBI's deadline of **Monday, July 9, 2012** for ensuring computers are not infected with the DNSChanger malware. This malware changes the default Domain Name System (DNS) server IP address on infected hosts to that of one of several DNS servers operated by criminals. The FBI seized 100 servers responsible for this attack, but rather than shut them down, they assigned their IP addresses to clean, temporary DNS servers. Since any infected computer will immediately be unable to access the Internet once the servers are shut down, time was needed to alert users to clean their computers and correct the DNS server IP address if needed. These FBI-maintained temporary DNS servers are still seeing traffic from over 70,000 US IP addresses indicating that not all users have done this. No extension of the July 9 deadline is expected. The FBI will most likely disable the temporary DNS servers at that time.

In addition, any computers that have been infected with the malware may have antivirus protection or automatic software updates disabled as a result.

The FBI has issued an instruction sheet to aid users in determining whether they are infected with this malware and how to correct the default DNS IP address. State users should depend on their IT department's instructions for any DNS corrections on state-owned machines. Home users may find assistance for checking and remediating their personally-owned computers in the links below.

More information:
http://www.dcwg.org

May 29, 2012 COT Security Alert "Deadline for Remediation of DNSChanger-Infected Hosts":
http://technology.ky.gov/COT%20Alerts/Deadline%20for%20Remediation%20of%20DNSChanger-Infected%20Hosts.pdf

FBI link:
http://www.fbi.gov/news/stories/2011/november/malware_110911/DNS-changer-malware.pdf

NOTICE: COT is providing this information so that you are aware of the latest security threats, vulnerabilities, software patches, etc. You should consult with your network administrator or other technical resources to ensure that the appropriate actions for these alerts are followed. If you are a network administrator and need additional information, please call the Help Desk at 502.564.7576.

Security Administration Branch
Commonwealth Office of Technology
120 Glenn's Creek Road, Jones Building
Frankfort, KY 40601
COTSecurityServicesISS@ky.gov
http://technology.ky.gov/security/